REMARKS

STATUS OF CLAIMS

Claims 1-20 have been pending.

The Drawings are objected to in view of the Specification, page 7, line 22, using reference number 56. According to the foregoing, the specification is amended to be consistent with FIG. 2 of the present Application. Withdrawal of the drawing objection is respectfully requested.

Claim 6 is objected to for missing a period. Claim 6 is amended taking into consideration the Examiner's comment. Withdrawal of the objection to claim 6 is respectfully requested.

Independent claims 1, 4, 6, 8, 9, 11 (including dependent claims 12-13), 14 (including dependent claims 15-16), and 17-19 are rejected under 35 USC 102(e) as being anticipated by Dykes (US Patent No. 5,872,915).

Independent claims 2, 3, 5, 7, 10, and 20 are rejected under 35 USC 103(a) as being unpatentable over Dykes in view of Cohen (US Patent No. 6,178,511).

Claims 1-5, 7, 9, 10 and 14-20 are cancelled without prejudice or disclaimer. Claims 6, 8 and 11-13 are amended.

Thus, claims 6, 8 and 11-13 remain pending for reconsideration, which is respectfully requested.

No new matter has been added in this Amendment. The forgoing rejections are hereby traversed.

CLAIM REJECTIONS

The independent claims 6, 8 and 11 are amended to emphasize the present invention's patentably distinguishing feature of an integrated circuit card (smart card) managing protected web page certificates as described on page 14, line 7 to page 16, line 15; and FIGS. 12-13 of the present Application (see, cancelled independent claims 3 and 20). See also, page 9, lines 11 of the present Application.

Claims 1-5, 7, 9, 10 and 14-20 are cancelled without prejudice or disclaimer.

Dykes

Dykes discloses a system for providing secure access to a software application from a web browser over the WWW. With reference to FIGS. 3 and 4, Dykes in column 3, lines 45-53 and column 9, lines 7-28, discloses a web browser 212 and gateway 332. In particular, in Dykes, column 3, lines 45-53, the user inputs data via the web browser, which is communicated to the web server application 222. The web server application 222 then authenticates the web browser 212, and passes appropriate input data to an application gateway 332, including data to uniquely identify the web browser 212. The application gateway 332 then uses authentication data received from the browser 212 to determine whether the user of the browser is authorized to access the software application 342. Further, in Dykes, the gateway 332 contains a user library that contains authentication data needed to access the corresponding software applications for each authorized user (column 9, lines 19-21).

Cohen

The Examiner relies on Cohen for the present invention's application certificates as recited in independent claims 6, 8 and 11. Cohen discloses a single sign-on (SSO) mechanism that coordinates logons to local and remote resources in a computer enterprise with preferably one ID and password (column 2, lines 24-27). In particular, Cohen discloses that the SSO framework supports storage of all passwords and keys belonging to a user in a secure storage (e.g., either in local storage, a centralized password service, a smart card, or the like), so that the user needs to remember only on ID and password (column 2, lines 33-41).

THE PRESENT CLAIMED INVENTION

The independent claims 6, 8 and 11 are amended to emphasize the present invention's patentably distinguishing feature of an integrated circuit card managing protected web page certificates as described on page 14, line 7 to page 16, line 15; and FIGS. 12-13 of the present Application (see, cancelled independent claims 3 and 20). See also, page 9, lines 11 of the present Application.

Independent claims 6, 8, and 11-13, using the recitation of claim 11 as an example, are amended as follows:

> 11. (CURRENTLY AMENDED) A user authentication ~~apparatus~~computer system, comprising:
>
> a computer, comprising:
>
> an integrated circuit card reader, and
>
> a programmed computer processor communicating with a network and executing a web browser processing a protected web page received from the network; and
>
> an integrated circuit card read by the integrated circuit card reader and storing a certificate to access the protected web page and characteristic identifying information of a user associated with the web page, and storing at least one program performing a process comprising:
>
> ~~a control unit controlling comparison of~~comparing identifying information input by ~~a~~the user with the user characteristic identifying information stored on the integrated circuit card, and ~~stored in a storage medium storing authentication information for applications corresponding to the characteristic identifying information; and~~
>
> in response to the comparing, providing the stored certificate to the web browser to access the received protected web page
>
> ~~a set unit setting in one of the applications selected by the user the authentication information the storage medium sends responsive to a result of the comparison to the set unit, as input information for authentication by the one selected application, wherein the control unit further comprises:~~
>
> ~~a providing unit providing the identifying information input by the user to the storage medium; and~~
>
> ~~a receiving unit receiving the result of the comparison the storage medium sends responsive to the result of the comparison; and wherein the storage medium further comprises a comparing unit comparing the input identifying information provided to the storage medium with the characteristic identifying information stored in the storage medium~~.

The Examiner relies on Cohen, column 6, lines 23-29 and 38-45, and column 4, lines 44-48, to reject the present invention's claimed use of application certificates. However, both Dykes and Cohen do not disclose or suggest using a certificate, such as a secret key, managed by an integrated circuit card and used to access a protected web page received and to be displayed by a WWW browser.

In other words, according to the present invention, when the web browser requests and receives an encrypted web page to be displayed, the web browser requests a certificate to decrypt the received encrypted web page. The integrated circuit card of the present invention manages and provides the certificates corresponding to encrypted web site applications that are sent to/received by the web browser and require decryption by the web browser.

In contrast to the present claimed invention, Dykes (with reference to FIGS. 3 and 4) discloses that the web browser 212 provides authentication information to the web server 222, and the web server 222 authenticates the web browser 212 (column 3, lines 35-41). Further, Cohen does not even mention the WWW as a network, and therefore does not disclose or suggest the present invention's claimed configuration of integrated circuit card (smart card) management of protected web page certificates and access to the protected web pages. Further, a combined Dykes and Cohen system would not disclose or suggest the present claimed invention, and it would not be obvious to one skilled in the art to modify a combined Dykes-Cohen system to achieve the present invention, because the Dykes implementation of a secure access to a software application from a web browser over the WWW involves the web browser 212 providing authentication information to the web server/application gateway/software application (222, 332 and 342), which differs from the present invention's "an integrated circuit card read by the integrated circuit card reader and storing a certificate to access the protected web page and characteristic identifying information of a user associated with the web page, ... comparing identifying information input by the user with the user characteristic identifying information stored on the integrated circuit card, and in response to the comparing, providing the stored certificate to the web browser to access the received protected web page."

In contrast, to Dykes and Cohen, the claimed invention provides authentication information, via an integrated circuit card, to a web browser to access a web page received and to be processed (e.g., displayed) by the web browser by reciting,

> 6. (CURRENTLY AMENDED) A process of user authentication, comprising:
>
> executing a web browser processing a protected web page received from the network;
>
> storing on an integrated circuit card a certificate to access the protected web page and characteristic identifying information of a user associated with the received protected web page;
>
> reading by an integrated circuit card reader the integrated circuit, in response to receipt of the protected web page by the web browser;
>
> comparing identifying information input by the user with the characteristic identifying information of the user stored in the integrated circuit card ; and
>
> in response to the comparing, providing the certificate stored on the integrated circuit card to the web browser to access the received protected web page.

In view of the claim amendments and the remarks, withdrawal of the rejections of claims 6, 8 and 11-13 and allowance of claims 6, 8, and 11-13 is respectfully requested.

DEPENDENT CLAIMS

Further the dependent claims 12 and 13 recite patentably distinguishing features of their own, as follows. In contrast to Dykes and Cohen, the present invention as recited in dependent claim 12 provides:

> 12. (CURRENTLY AMENDED) The computer system of claim 11, wherein the computer further comprises a display unit and the integrated circuit card program further performs:
>
> displaying on the display unit selectable names of protected applications as protected web pages, if a result of the comparing of the user identifying information is matching; and
>
> the providing of the stored certificate comprises providing one of a plurality of certificates stored on the integrated circuit card and corresponding to a selected one of the protected applications by the user to the web browser to access the selected protected application.

Further, in contrast to Dykes and Cohen, the present invention as recited in dependent claim 13 provides:

> 13. (CURRENTLY AMENDED) The computer system of claim 12, wherein the integrated circuit card stores information about the protected applications and the selectable names of the protected applications are provided to be displayed on the display unit, if the result of the comparing of the user identifying information is matching.

CONCLUSION

There being no further outstanding objections or rejections, it is submitted that the application is in condition for allowance. An early action to that effect is courteously solicited.

Finally, if there are any formal matters remaining after this response, the Examiner is requested to telephone the undersigned to attend to these matters.

Respectfully submitted,
STAAS & HALSEY LLP

Date: April 19, 2004

By: _____
Mehdi D. Sheikerz
Registration No. 41,307

1201 New York Avenue, NW, Suite 700
Washington, D.C. 20005
Telephone: (202) 434-1500
Facsimile: (202) 434-1501